Quantum-Safe Message Authentication for Industrial IOT using “QKDLite” with LPN

Teik Guan Tan, Shi Hong Choy
pQCee Pte Ltd

Yu Xiang Peh, Syed Abdullah Aljunid, Christian Kurtseifer
S-Fifteen Instruments Pte Ltd

Introduction

Quantum Key Distribution (QKD) can be used by communicating parties to exchange a random and secret key. While many projects have worked on using QKD to achieve data confidentiality, we design a novel usage of QKD to achieve secure user and message authentication. This is done by combining QKD with Learning Parity with Noise (LPN) into a simple and lightweight message authentication algorithm which is quantum-secure and not susceptible to tampering or man-in-the-middle attacks.

We implement this algorithm to provide quantum-safe data integrity and device authentication for an Industrial Internet of Things (IIoT) setup running over the MODBUS protocol. The QKD modules are further optimized for cost into a Spontaneous Parametric Down Conversion (SPDC) or "QKDLite" package by removing much of the unneeded polarization and error-correction circuitry. A demonstration of this IIoT setup is shown where a supervisory control and data acquisition (SCADA) system will communicate securely with a programmable logic controller (PLC) while connected to their respective QKDLite modules. We show that this setup costs less than 30% of a regular QKD implementation, while the communication and processing overheads is also reduced by 80% as compared to using post-quantum cryptographic techniques.

This setup can be further adapted to support new use-cases such as Remote User-Password Verification as well as Secure Broadcasting.

Learning Parity with Noise (LPN)

LPN is a post-quantum cryptographic system with low memory and computational requirements which makes it useful as a cryptosystem for low-resource devices. LPN has its roots in code-based cryptography and can also be seen as a special case of a lattice-based Learning-with-Error (LWE) problem, both of which are still being evaluated by NIST as possible candidates for PQC standardization. The Hopper-Blum (HB) protocol (see Figure 1) is an application of the LPN cryptosystem to allow two communicating parties to use a challenge-response method to authenticate each other.

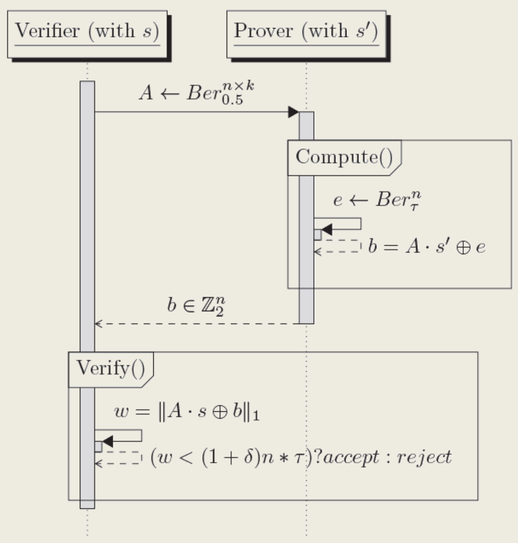

Figure 1 – Hopper-Blum Protocol over Learning Parity with Noise

While HB is shown to be secure against passive attackers who cannot influence or change the challenge, it is insecure against active adversaries who can modify or fake the challenge. This can be solved by relying on a distributed random source to generate the challenge.

Spontaneous Parametric Down Conversion (SPDC)

SPDC is the key component required for most entanglement-based QKD. The production of photons via SPDC is an inherently random process in time, but the simultaneous pairs of photons generated have a very special property of time correlation which we can use to generate identical random bits at two distant locations. This is accomplished when we send each of the pair of single photons to different distant locations, and their arrival time measured. After post-processing the timing information, we obtain the generated random bits or “challenge” that can then be fed into the HB protocol at the two parties to establish “quantum-safe” communication.

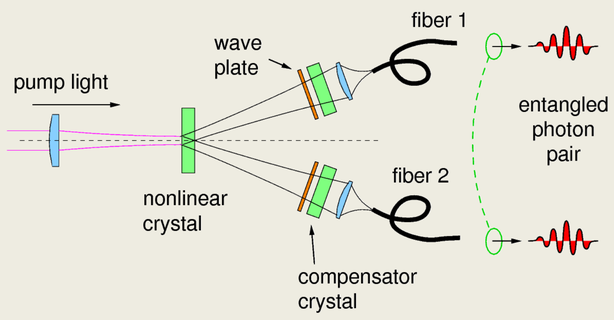

Figure 2 – Spontaneous Parametric Down Conversion

SPDC as a distributed random source

Photon pairs of wavelength centered at 810 nm are generated via a Type-I spontaneous parametric down-conversion (SPDC) process in a Beta-Barium Borate (β-BBO) crystal. The photon pairs are strongly time-correlated (to within ~fs of each other) and are separated for detection by both Alice and Bob respectively using single photon sensitive Silicon avalanche photodetectors (APDs). Simultaneous detection on both detectors, after accounting for propagation delays through the optical fibers, corresponds to the likely detection of a photon pair. The detection pulses fired by the APDs are assigned timestamps by a time tagger with a timing resolution of 2 ns.

The detection time interval between successive detections of photon pairs on each side is inherently probabilistic due to the nature of the SPDC process and follows that of a Poisson distribution with a mean corresponding to the average discretized waiting time. Due to the presence of additional noise counts (e.g. APD dark counts, non-unity optical transmission, detector efficiency), a two-way communication protocol `qcrypto` is performed between Alice and Bob to agree on the timestamps corresponding to a coincidence detection. This protocol itself is responsible for identifying the propagation delay corresponding to the photon pairs (with an accuracy of ~ns), compensation of frequency difference between clocks on both parties, and performing active frequency compensation of clock drift.

The timing differences obtained from the set of agreed timestamps follow the Poisson distribution; an inverse transform is performed to map these timing differences to a uniform distribution, with the number of bits available for extraction given by the Shannon entropy. An additional round of hashing using SHA-256 is performed to remove any residual timing correlations (e.g. from detector afterpulsing), before being sent as a bitstream to a pipe for consumption by downstream applications. This extraction protocol is described by Wayne et. al. [3]

QKDLite Authentication for MODBUS

For this project, we work on MODBUS v1.1a (2004) [1] . MODBUS works on a Client-Server model where the SCADA Client sends a request to the PLC Server which then returns with a response. For TCP/IP communications, a 7-byte MODBUS Application Protocol (MBAP) header is added to the Protocol Data Unit (PDU) made up of Function Code (1 byte) and Data (up to 252 bytes) for a maximum size of 260 bytes.

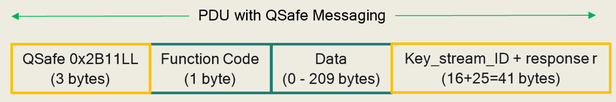

Figure 3 – Added Qsafe wrapper over the MODBUS PDU

We next built in-line proxy modules to carry out the QKDLite authentication on behalf of the MODBUS Client and Server. The parameters we have chosen for our HB-LPN implementation [2] are:

- Noise τ = 0.125 Size of secret s = 64 bits
- Number of rows r = 200 Authentication window δ = 0.8

This will reduce the allowed Data from the original (0 to 252) bytes, to (0 to 209) bytes. See Figure 3.

The architecture is shown in Figure 4 where we custom build a SCADA application as the Client and used OpenPLCv3 as the Server.

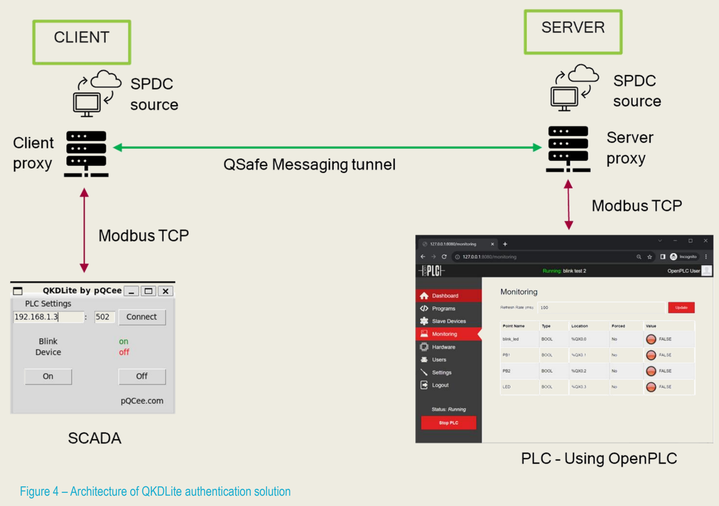

Figure 4 – Architecture of QKDLite authentication solution

Performance

We compare the data size and performance overheads of running QKDLite authentication (using HB-LPN) versus Dilithium, a NIST-PQC candidate.

	QKDLite Authentication	Dilithium NIST PQC Signatures	Improvement
Data overhead	41 bytes	2420 bytes	98%
Proof Generation (CPU cycles)	22715 cycles	141138 cycles	83%
Proof Verification (CPU cycles)	10919 cycles	55533 cycles	80%

Solution Setup

We provide an actual setup in Figure 5 of how 2 Raspberry Pis, functioning as the SCADA client and PLC server respectively, can perform MODBUS communication securely using the QKDLite setup.

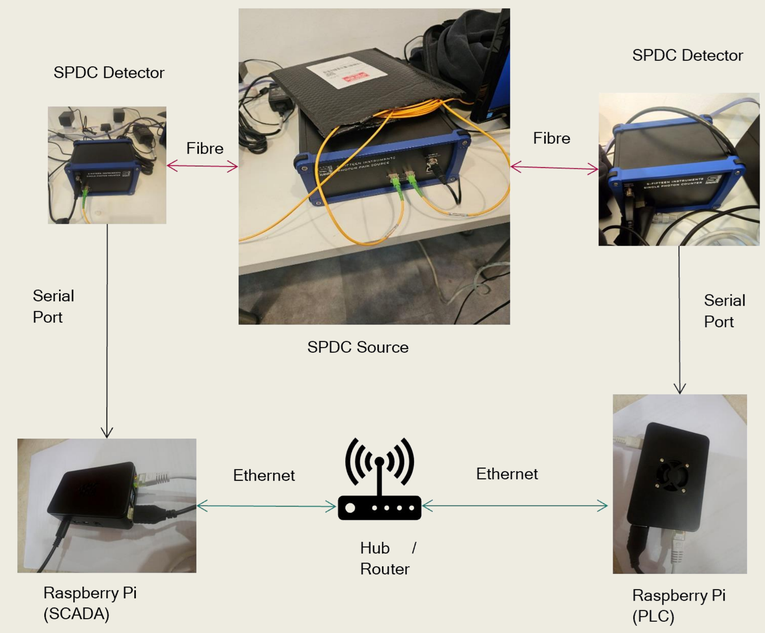

Figure 5 – Industrial IOT setup of a SCADA Raspberry Pi communicating to a PLC Raspberry Pi protected with QKDLite

The distance between the 2 SPDC Detectors is 10 metres. Under ambient room lighting (See Figure 6), we achieved transmission rate of 3 MODBUS messages / second.

Figure 6 – From left, Syed,Yu Xiang and Teik Guan in actual lighting conditions during testing

Conclusion

Threat of quantum computers will change how secure communications happen in the near future. We have successfully demonstrated how quantum-safe messaging for low-resource systems such as Industrial IOT can be achieved by combining elements of quantum communications with quantum-safe cryptography.

Acknowledgements

This project is partially supported by Enterprise Singapore STARTUP SG TECH – PROOF-OF-CONCEPT (POC) Grant

This setup incorporates certain features that may be subject to claims in pQCee's patent-pending application (PCT WO2024049352).

References

[1] Modbus.org, “MODBUS APPLICATION PROTOCOL SPECIFICATION V1.1a”, Available at: https://www.modbus.org/docs/Modbus_Application_Protocol_V1_1a.pdf

[2] Tan, Teik Guan, De Wen Soh, and Jianying Zhou. "Calibrating Learning Parity with Noise Authentication for Low-Resource Devices." In International Conference on Information and Communications Security, pp. 19-36. Cham: Springer International Publishing, 2022.

[3] Wayne, Michael A., Evan R. Jeffrey, Gleb M. Akselrod, and Paul G. Kwiat. “Photon Arrival Time Quantum Random Number Generation.” Journal of Modern Optics 56, no. 4 (February 20, 2009): 516–22. https://doi.org/10.1080/09500340802553244.

Contact Information

Teik Guan Tan

pQCee Be . Quantum . Ready

Tel: +65 9746 9386
@tanteikg

Email: teikguan@pqcee.com
Web: www.pqcee.com